



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
GABINETE DA REITORIA

PORTARIA Nº 252, DE 12 DE MAIO DE 2021

Institui e regulamenta o funcionamento do Comitê de Resposta a Incidentes de Segurança da Informação - Crisi, no âmbito da Ufersa.

A Reitora da Universidade Federal Rural do Semi-Árido, no uso de suas atribuições conferidas pelo Decreto de 21 de agosto de 2020, publicado na edição extra no Diário Oficial da União de 21 de agosto de 2020; o artigo 44, incisos VI e XIX, do Estatuto da Universidade; o Decreto nº 2.014, de 26 de setembro de 1996; a competência que lhe foi subdelegada pela Portaria MEC nº 1.048, de 14 de outubro de 1996, publicada no Diário Oficial da União de 15 de outubro de 1996; a Resolução Consuni/Ufersa nº 15/2017, que institui a Política de Segurança da Informação e Comunicações no âmbito da Ufersa; o disposto no inciso V do artigo 5º da Instrução Normativa nº 1 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal; a Portaria nº 38/GSIPR, de 14 de agosto de 2009, que homologa a Norma Complementar nº 05/IN01/DSIC/GSIPR; a Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 04 de agosto de 2009, que disciplina a criação de Equipe de Tratamento de Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF; a Portaria nº 57/GSIPR, de 23 de agosto de 2010, que homologa a Norma Complementar nº 08/IN01/DSIC/GSIPR; a Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 19 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF; a Portaria nº 40, de 8 de outubro de 2014, que homologa a Norma Complementar nº 21/IN01/DSIC/GSIPR, publicada no Diário Oficial da União de 10 de outubro de 2014; o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional, resolve:

Art. 1º Instituir o Comitê de Resposta a Incidentes de Segurança da Informação – Crisi/Ufersa, em observância à Política de Segurança da Informação e Comunicações da Ufersa, conforme definido a seguir.

Parágrafo único. O regimento interno do Crisi/Ufersa que regulamenta o funcionamento da equipe está disposto no Anexo I.



**MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
GABINETE DA REITORIA**

Art. 2º O Comitê de Resposta a Incidentes de Segurança da Informação – Crisi/Ufersa, será composto pelos servidores:

I – Diretor (a) da Divisão de Segurança da Informação:

b) Alex José Velasco Nunes.

II – Membro da Divisão de Segurança da Informação:

c) Kleber Jacinto – Analista de Tecnologia da Informação – Titular; e

d) João Phellipe de Freitas Pinto - Analista de Tecnologia da Informação – Suplente.

III – Membro da Divisão de Infraestrutura Computacional:

c) Marcelo Carlos Araújo - Analista de Tecnologia da Informação – Titular; e

d) Igor Saraiva Brasil - Analista de Tecnologia da Informação – Suplente.

IV – Membro da Divisão de Sistemas Computacionais:

c) Vially Israel Lopes Aragão - Técnico de Tecnologia da Informação – Titular, e

d) Marcos Tullyo Campos – Analista de Tecnologia da Informação – Suplente.

V – Membro da Divisão de Suporte e Serviços:

c) Christien Antunes Pinheiro F. de Andrade - Técnico de Tecnologia da Informação – Titular, e

d) Alisson Alan Lima da Costa – Técnico de Tecnologia da Informação – Suplente.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

LUDIMILLA CARVALHO SERAFIM DE OLIVEIRA



**MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
GABINETE DA REITORIA**

ANEXO I

REGIMENTO INTERNO DO CRISI

CAPÍTULO I

MISSÃO E VISÃO

Art. 1º O Comitê de Resposta a Incidentes de Segurança da Informação – Crisi/Ufersa tem por missão coordenar e gerenciar atividades de prevenção, tratamento e resposta a incidentes de segurança da informação na rede de computadores da Ufersa, preservando os dados, informações e infraestrutura, além de promover ações de disseminação de conhecimento aos seus colaboradores sobre uso seguro dos recursos computacionais.

Art. 2º A visão do Crisi/Ufersa é ser a referência organizacional para violações de dados, atuando na resposta a incidentes de segurança da informação em redes de computadores para a comunidade técnica interna e instituições externas, buscando fortalecer a prevenção e detecção de incidentes de segurança da informação.

CAPÍTULO II

PÚBLICO ALVO

Art. 3º A abrangência das atividades pertinentes ao Crisi/Ufersa inclui:

- I - Superintendência de Tecnologia da Informação e Comunicação – Sutic/Ufersa e os equipamentos sob sua responsabilidade distribuídos no Campus Central;
- II - Equipamentos sob tutela da Sutic/Ufersa nos campi fora da sede; e
- III - Os ativos de tecnologia da informação e serviços computacionais sob administração e tutela da Ufersa, não fazendo parte do escopo equipamentos ou serviços de terceiros.

Art. 4º O contato com o Crisi/Ufersa, para fins de envio e recebimento de notificações de incidentes de rede computacional, e outras comunicações institucionais, deve ser realizado através da conta de e-mail crisi@ufersa.edu.br.

Art. 5º As atividades devem ser realizadas com o intercâmbio de informações e em cooperação com as seguintes organizações:



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
GABINETE DA REITORIA

I - Centro de Tratamento a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV;

II - Equipes de resposta a tratamento de incidentes da informação e comunicações dos demais órgãos da Administração Pública Federal;

III - Centro de Atendimento a Incidentes de Segurança - CAIS/RNP;

IV - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br; e

V - Órgãos, entidades, empresas públicas ou privadas que tenham contratos, acordos ou convênios com a Ufersa.

CAPÍTULO III
SERVIÇOS

Art. 6º O Crisi/Ufersa deve prover os seguintes serviços ao seu público:

I - Tratamento de incidentes de segurança, que tem como propósito coordenar as ocorrências de incidentes de redes computacionais e acompanhar as ações de tratamento e resposta perante a SUTIC/UFERSA e o Comitê Governança Digital - CGD/Ufersa;

II - Gerenciamento de vulnerabilidades, com a finalidade de identificar falhas de segurança em ativos, serviços e sistemas, analisando, em conjunto com as unidades, as vulnerabilidades e orientando sua mitigação antes da exploração por agentes maliciosos;

III - Monitoramento de segurança da rede, com o objetivo de monitorar fluxos de tráfego de rede para identificação de sinais de atividade maliciosa; e

IV - Disseminação da cultura em segurança da informação, com o escopo de promover educação e treinamento para colaboradores da Ufersa sobre as melhores práticas de segurança da informação no âmbito da TI.

§ 1º O atendimento dos serviços previstos nos incisos I, II e IV deste artigo ocorrerá no horário de funcionamento da Sutica/Ufersa.

§ 2º O monitoramento previsto no inciso III deste artigo será automatizado acontecendo 24 horas por dia, 7 dias por semana.

CAPÍTULO IV
MODELO ORGANIZACIONAL



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
GABINETE DA REITORIA

Art. 7º O Crisi/Ufersa deve adotar o modelo Equipe de TIC.

§ 1º Os membros do Crisi/Ufersa não devem atuar com dedicação exclusiva às atividades da equipe, devendo desempenhar suas funções regulares na Ufersa e, em conjunto, com as atividades relacionadas à gestão do processo de tratamento e resposta aos incidentes em redes computacionais.

§ 2º Todas as Divisões da Sutic/Ufersa devem estar representadas no Crisi/Ufersa através de membros integrantes do comitê.

§ 3º As atividades relacionadas à execução do tratamento dos incidentes nos campi fora da sede podem ser apoiadas por servidores lotados nos campi, sem a necessidade de integrá-los à equipe do comitê.

CAPÍTULO V
ESTRUTURA ORGANIZACIONAL

Art. 8º O Crisi/Ufersa será vinculado à Superintendência de Tecnologia da Informação e Comunicação – Sutic/Ufersa.

Art. 9º O Crisi/Ufersa será composto pelos seguintes representantes, todos da Sutic/Ufersa:

- I - Diretor (a) da Divisão de Segurança da Informação;
- II - Membro da Divisão de Segurança da Informação;
- III - Membro da Divisão de Infraestrutura Computacional;
- IV - Membro da Divisão de Sistemas Computacionais; e
- V - Membro da Divisão de Suporte e Serviços.

§ 1º A presidência do Crisi/Ufersa será exercida pelo Diretor(a) da Divisão de Segurança da Informação e, em seus afastamentos ou impedimentos legais, assumirá o membro da Divisão de Segurança da Informação.

Art. 10. O Crisi/Ufersa deve ser composto por profissionais com conhecimento e experiência técnica compatíveis com a importância e missão da equipe e de seus respectivos cargos.

Art. 11. O Agente Responsável do Crisi/Ufersa deve ser designado pelo Gestor de Segurança da Informação da Ufersa, devendo ser um servidor público efetivo da Ufersa.

Parágrafo único. São responsabilidades do Agente Responsável do Crisi/Ufersa:

I - Responder pela coordenação do Crisi/Ufersa, gerenciar as atividades de seus membros, bem como coordenar metodologias e procedimentos internos;



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
GABINETE DA REITORIA

II - Representar o Crisi/Ufersa em reuniões e foros internos com a Reitoria, o CGD/UFERSA, e/ou outras instâncias internas da Ufersa;

III - Ser interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR Gov;

IV - Ser interface junto às autoridades policiais e judiciais competentes sobre incidentes de rede computacionais que tipifiquem crime;

V - Responder por todas as decisões, ações técnicas e administrativas do Crisi/Ufersa; e

VI - Apresentar relatórios executivos sobre os incidentes de rede computacionais e atividades do Crisi/Ufersa.

Art. 12. Os membros do Crisi/Ufersa devem ser servidores efetivos do quadro funcional da Ufersa.

§ 1º Para cada membro titular do Crisi/Ufersa que compõe a equipe, deve ser indicado um suplente correspondente.

§ 2º São responsabilidades de cada um dos membros do Crisi/Ufersa:

I - Responder às notificações de incidentes de rede computacional encaminhadas à Ufersa;

II - Notificar outras equipes de resposta à incidentes de segurança quando identificado um ataque cibernético direcionado à Ufersa;

III - Validar a resolução dos incidentes de rede e a recuperação do ambiente computacional após o incidente, analisando a causa raiz dos incidentes e vulnerabilidades e recomendar ações para evitar reincidências;

IV - Manter a base de dados de informações de incidentes e vulnerabilidades sempre consistentes e atualizadas;

V - Preservar evidências e artefatos maliciosos quando necessário;

VI - Propor sugestões e melhorias de processos de tratamento de incidentes de redes computacionais;

VII - Reportar todas as atividades do CRISI/UFERSA para o Agente Responsável;

VIII - Auxiliar o Agente Responsável, quando requisitado ou necessário, em tomadas de decisão; e

IX - Gerar relatórios técnicos sobre os incidentes e vulnerabilidades computacionais e atividades do Crisi/Ufersa.

CAPÍTULO VI



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
GABINETE DA REITORIA
AUTONOMIA

Art. 13. O Crisi/Ufersa não deve ter autonomia para intervir no ambiente computacional das respectivas unidades da Ufersa.

§ 1º O Crisi/Ufersa pode recomendar procedimentos a serem executados ou medidas de recuperação para impedir ou mitigar, ressalvando o caráter sugestivo das recomendações.

§ 2º O Crisi/Ufersa deve manter uma base de dados atualizada de erros conhecidos, políticas e procedimentos técnicos, podendo se valer de boas práticas de mercado, desde que não conflitem com dispositivos legais em vigor.

§ 3º O Crisi/Ufersa pode executar procedimentos ou medidas de recuperação durante um incidente, sem sobrepor-se às demais ações da Sutic/Ufersa.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 14. O Crisi/Ufersa deve levar assuntos de interesse relevante à Sutic/Ufersa e ao CGD/Ufersa, visando, principalmente, a prevenção de novos incidentes de redes computacionais.

Art. 15. Casos omissos devem ser resolvidos pelo Agente Responsável, em observância à Política de Segurança da Informação da Ufersa e da legislação em vigor.